IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): A method of encrypting an input data string including a plurality of bits of binary data with a processing device communicatively coupled to a memory having executable instructions stored therein which cause the processing device to implement a method of encryption, the method comprising:

receiving the input data string for encryption at the processing device;

providing a control code index in the memory, the control code index being defined prior to encryption at the processing device, the control code index including a plurality of control codes each defining respective orders of n bit combinations of binary data;

determining an order in which to query the presence of each of 2^n different configurations of n bits within the input data string;

~~generating~~ identifying a control code associated with the determined order using the control code index~~, the generated control code being selected from the control code index independent of specific characteristics of the input data string~~;

generating a position code ~~by identifying~~ using the identified control code in cooperation with a position code routine associated with the identified control code to determine positions of each of the 2^n different configurations of n bits in the input data string ~~in accordance with the determined order~~by comparing the 2^n different configurations of the input data string with the associated 2^n bit configurations of the identified control code, the comparisons resulting in output values dictated by the position code routine which defines the generated position code; and

combining the identified control code and the generated position code as components of an encrypted data string.

Claim 2 (Canceled).

Claim 3 (Previously Presented): The method of Claim 1, wherein determining an order comprises selecting a predetermined order.

Claim 4 (Canceled).

Claim 5 (Previously Presented): The method of Claim 1, further comprising:

dividing the input data string into a plurality of blocks of data.

Claim 6 (Previously Presented): The method of Claim 5, wherein the number of bits within each of the plurality of blocks of data is individually determined in response to a random number generator.

Claim 7 (Previously Presented): The method of Claim 5, wherein the number of bits within each of the plurality of blocks of data is individually determined in accordance with a rule set.

Claim 8 (Previously Presented): The method of Claim 5, further comprising:

generating a plurality of block codes associated with a plurality of blocks of data of the input data string, each block code indicating the number of bits within the associated block of data.

Claim 9 (Currently Amended): The method of Claim 8, further comprising:

combining ~~the~~ each of the plurality of block codes with the identified control code and the generated position code for the associated block of data.

Claim 10 (Currently Amended): The method of Claim 1, wherein determining an order further comprises:

determining an order based on the frequencies of the 2^n combinations of the n bits of the input data string.

Claims 11-20 (Canceled).

Claim 21 (Currently Amended): A method for encrypting an input data string, including a plurality of bits of binary data, the method comprising:

receiving the input data string for encryption;

providing a control code index , the control code index being defined prior to encryption, the control code index including a plurality of control codes each defining respective orders of n bit combinations of the input data string;

determining an order in which to query the presence of each of 2^n different configurations of n bits within the input data string;

~~generating~~ identifying a control code associated with the determined order using the control code index~~, the generated control code being selected from the control code index independent of specific characteristics of the input data string~~;

generating a position code ~~by identifying~~ using the identified control code in cooperation with a position code routine associated with the identified control code to determine positions of each of the 2^n different configurations of n bits in an input data string ~~in accordance with the determined order~~by comparing the 2^n different configurations of the input data string with the associated 2^n bit configurations of the identified control code, the

comparisons resulting in output values dictated by the position code routine which defines the generated position code; and

combining the identified control code and the generated position code as components of an encrypted data string.

Claim 22 (Previously Presented): The method of Claim 21, further comprising arranging the input data string into a plurality of data blocks.

Claim 23 (Currently Amended): A computer readable medium including computer program instructions that cause a computer to implement a method of encrypting ~~the~~ an input data string, including a plurality of bits of binary data, the method comprising:

receiving the input data string for encryption;

providing a control code index that is defined prior to encryption, the control code index including a plurality of control codes each defining respective orders of n bit combinations of binary data;

determining an order in which to query the presence of each of 2^n different configurations of n bits within the input data string;

~~generating~~ identifying a control code associated with the determined order using the control code index~~, the generated control code being selected from the control code index independent of specific characteristics of the input string~~;

generating a position code ~~by identifying~~ using the identified control code in cooperation with a position code routine associated with the identified control code to determine the positions of each of the 2^n different configurations of n bits in the input data string ~~in accordance with the determined order~~by comparing the 2^n different configurations of the input data string with the associated 2^n bit configurations of the identified control code,

the comparisons resulting in output values dictated by the position code routine which defines the generated position code; and

combining the identified control code and the generated position code as components of an encrypted data string.

Claim 24 (Canceled).

Claim 25 (Previously Presented): The method of Claim 23, wherein determining an order includes selecting a predetermined order.

Claim 26 (Previously Presented): The method of Claim 23, further comprising :

dividing the input data string into a plurality of blocks of data.

Claim 27 (Previously Presented): The method of Claim 26, wherein dividing the input data string into a plurality of blocks of data includes determining the individual number of bits within each of the plurality of blocks of data in response to a random number generator.

Claim 28 (Previously Presented): The method of Claim 26, wherein dividing the input data string into a plurality of blocks of data, includes determining the individual number of bits within each of the plurality of blocks of data in accordance with a rule set.

Claim 29 (Previously Presented): The method of Claim 26, wherein determining an order further comprises:

determining a first order associated with a first block of data and determining a second order associated with a second block of data wherein the first order is different than the second order.

Claim 30 (Previously Presented): The method of Claim 26, further comprising:

generating a plurality of block codes associated with a plurality of blocks of data, each block code indicating the number of bits within the associated block of data.

Claim 31 (Currently Amended): The method of Claim 30, further comprising:

combining the each of the plurality of block codes with the identified control code and the generated position code for the associated block of data.

Claim 32 (Previously Presented): The method of Claim 23, wherein determining an order includes determining an order based on the frequencies of the 2^n combinations of the n bits of the input data string.

Claim 33 (Previously Presented): The method of Claim 23, wherein determining an order includes determining an order in which to query the presence of each of 2^n different configurations of n bits based on an analysis of the input data string.

Claim 34 (Currently Amended): The method of Claim 23, wherein ~~generating~~ identifying the control code includes randomly selecting the control code via a random number generator.

Claim 35 (Previously Presented): The method of Claim 23, wherein determining an order includes generating an order using a rule set.

Claim 36 (Currently Amended): The method of Claim 23, further comprising:

determining whether to compress the input data string ~~can be compressed~~ simultaneously as it is encrypted.

Claim 37 (Currently Amended): The method of Claim ~~23~~32, further comprising:

dividing the input data string into n bit sequences;

comparing each of the 2^n different configurations of n bits of binary data with each of the n bit sequences;

determining the frequency of each of the 2^n different configurations appearing in the input data string;

determining whether a specific relationship exists between values of the frequencies of each of the individual 2^n different configurations appearing in the input data string wherein the existence of the specific relationship is indicative of the presence of a characteristic within the input data string and wherein the presence of the characteristic ~~indicates~~ determines that the input data string ~~can be~~ is compressed simultaneously as it is encrypted;

selecting a first position code routine associated with the determined order when the specific relationship exists, the first position code routine being operable to simultaneously encrypt and compress the input data string; and

selecting a second position code routine associated with the determined order when the specific relationship does not exist, the second position code routine being operable to encrypt the input data string without any compression.

Claim 38 (Currently Amended): The method of Claim ~~23~~37, wherein determining the order in which to query the presence of each of 2^n different configurations of n bits of binary data within an input data string includes determining the order in which to query the presence of each of 4 different configurations of 2 bits within an input data string.

Claim 39 (Currently Amended): The method of Claim 38, further comprising:

dividing the input data string into n bit sequences;

comparing each of the 2^n different configurations of n bits of binary data with each of the n bit sequences of the input data string;

determining a first number representative of the number of times the most frequency occurring 2^n configuration appears in the input string.

determining a second number representative of the number of times the second most frequency occurring 2^n configuration appears in the input string;

determining a third number representative of the number of times the third most frequency occurring 2^n configuration appears in the input string;

determining a fourth number representative of the number of times the fourth most frequency occurring 2^n configuration appears in the input string;

determining an order in which to query the presence of each of 2^n different configurations of n bits within the input data string based on a sequence of 2 bit combinations, the determined order beginning with a most occurring frequency and ending with a least occurring frequency;

selecting a first position code routine associated with the determined order when the first number is greater than the sum of the third number and the fourth number thereby indicating the presence of a characteristic that indicates that the input data string can be

simultaneously encrypted and compressed, the first position code routine being operable to simultaneously encrypt and compress the input data string; and

selecting a second position code routine associated with the determined order when the first number is not greater than the sum of the third number and the fourth number thereby indicating the absence of the characteristic that indicates that the input data string can be simultaneously encrypted and compressed, the second position code routine being operable to encrypt the input data string without any compression.

Claim 40 (Currently Amended): The method of Claim 39, wherein ~~generating~~ identifying a control code associated with the determined order, further comprises:

~~generating~~ identifying a first control code associated with the determined order when the first position code routine is selected; and

~~generating~~ identifying a second control code associated with the determined order when the second position code routine is selected wherein the first control code is different than the second control code.

Claim 41 (Previously Presented): The method of Claim 23, further comprising encrypting the encrypted data string.

Claim 42 (Previously Presented): The method of Claim 41, wherein encrypting the encrypted data string comprises:

providing an encryption key having a first selected number of bits; and

performing an XOR function between the encryption key and the encrypted data string.

Claim 43 (Currently Amended): The method of Claim 41, wherein encrypting the encrypted data string comprises:

~~determining an order in which to query the presence of each of 2^n different configuration of n bits with the encrypted data string;~~

~~generating a control code associated with the determined order of the encrypted data string;~~

~~generating a position code by identifying the positions of each of the 2^n different configurations of n bits in the encrypted data string in accordance with the determined order; and~~determining an order in which to query the presence of each of 2^n different configurations of n bits within the input data string;

identifying a second control code associated with the determined order using the control code index each control code defining respective orders of n bit combinations of binary data;

generating a position code using the identified control code in cooperation with a position code routine associated with the identified control code to determine positions of each of the 2^n different configurations of n bits in the input data string by comparing the 2^n different configurations of the input data string with the associated 2^n bit configurations of the identified control code, the comparisons resulting in output values dictated by the position code routine which defines the generated position code; and

combining the second identified control ~~position~~ code and the ~~newly~~ second generated ~~control~~ position code to create a different encrypted version of the encrypted data string.

Claim 44 (Currently Amended): The method of Claim 25, wherein selecting a predetermined order includes ~~computer readable code for~~ selecting a default order.

Claim 45 (Previously Presented): The method of Claim 32, wherein determining an order based on the frequencies of the 2^n combinations of the n bits of the input data string includes determining an order based on the relative frequencies of the 2^n combinations of the n bits of the input data string.

Claim 46 (Cancelled).

Claim 47 (Currently Amended): The method of Claim 1, wherein ~~determining~~ identifying an order includes determining an order in which 2^n different configurations of n bits are to be identified in a position code based on an analysis of the input data string.

Claim 48 (Currently Amended): The method of Claim 1, wherein ~~generating~~ identifying the control code includes randomly selecting the control code via a random number generator.

Claim 49 (Previously Presented): The method of Claim 1, wherein determining an order includes generating an order using a rule set.

Claim 50 (Previously Presented): The method of Claim 5, wherein determining an order includes determining a first order associated with a first block of data and determining a second order associated with a second block of data wherein the first order is different than the second order.

Claim 51 (Currently Amended): The method of Claim 1, further comprising:

determining whether to compress the input data string ~~can be compressed~~ simultaneously as it is encrypted.

Claim 52 (Currently Amended): The method of Claim 1, further comprising:

dividing the input string into n bit sequences;

comparing each of the 2^n different configurations of n bits of binary data with each of the n bit sequences;

determining the frequency of each of the 2^n different configurations appearing in the input data string;

determining whether a specific relationship exists between values of the frequencies of each of the individual 2^n different configurations appearing in the input data string wherein the existence of the specific relationship is indicative of the presence of a characteristic within the input data string and wherein the presence of the characteristic ~~indicates~~ determines that the input data string ~~can be~~ is compressed simultaneously as it is encrypted;

selecting a first position code routine associated with the determined order when the specific relationship exists, the first position code routine being operable to simultaneously encrypt and compress the input data strong; and

selecting a second position code routine associated with the determined order when the specific relationship does not exist, the second position code routine being operable to encrypt the input data string without any compression.

Claim 53 (Previously Presented): The method of Claim 1, wherein determining the order in which to query the presence of each of 2^n different configurations of n bits within an input data string includes determining the order in which to query the presence of each of 4 different configurations of 2 bits within an input data string.

Claim 54 (Currently Amended): The method of Claim 53, further comprising:

dividing the input data string into n bit sequences;

comparing each of the 2^n different configuration of n bits of binary data with each of the n bit sequences of the input data string;

determining a first number representative of the number of times the most frequency occurring 2^n configuration appears in the input string;

determining a second number representative of the number of times the second most frequency occurring 2^n configuration appears in the input string;

determining a third number representative of the number of times the third most frequently occurring 2^n configuration appears in the input string;

determining a fourth number representative of the number of times the fourth most frequency occurring 2^n configuration appears in the input string;

determining an order in which to query the presence of each of 2^n different configurations of n bits within the input data string based on a sequence of 2 bit combinations, the determined order beginning with a most occurring frequency and ending with a least occurring frequency;

selecting a first position code routine associated with the determined order when the first number is greater than the sum of the third number and the fourth number thereby indicating the presence of a characteristic that indicates that the input data string can be simultaneously encrypted and compressed, the first position code routine being operable to simultaneously encrypt and compress the input data string; and

selecting a second position code routine associated with the determined order when the first number is not greater than the sum of the third number and the fourth number thereby indicating the absence of a characteristic that indicates that the input data string can

be simultaneously encrypted and compressed, the second position code routine being operable to encrypt the input data string without any compression.

Claim 55 (Currently Amended): The method of Claim 54, wherein ~~generating~~ identifying a control code associated with the determined order, further comprises:

~~generating~~ identifying a first control code associated with the determined order when the first position code routine is selected; and

~~generating~~ identifying a second control code associated with the determined order when the second position code routine is selected wherein the first control code is different than the second control code.

Claim 56 (Previously Presented): The method of Claim 1, further comprising: performing a further encryption of the encrypted data string.

Claim 57 (Previously Presented): The method of Claim 56, wherein performing a further encryption of the encrypted data string, further comprises:

providing an encryption key having a first selected number of bits; and

performing an XOR function between the encryption key and the encrypted data string.

Claim 58 (Currently Amended): The method of Claim 56, wherein performing a further encryption of the encrypted data, further comprises:

~~determining an order in which to query the presence of each of 2^n different configurations of n bits within the encrypted data string;~~

~~generating a control code associated with the determined order for the encrypted data string;~~

~~generating a position code by identifying positions of each of the 2^n different configurations of n bits in the encrypted data string in accordance with the determined order; and~~determining an order in which to query the presence of each of 2^n different configurations of n bits within the input data string each control code defining respective orders of n bit combinations of binary data;

identifying a second control code associated with the determined order using the control code index;

generating a position code using the identified control code in cooperation with a position code routine associated with the identified control code to determine positions of each of the 2^n different configurations of n bits in the input data string by comparing the 2^n different configurations of the input data string with the associated 2^n bit configurations of the identified control code, the comparisons resulting in output values dictated by the position code routine which defines the generated position code; and

combining the ~~newly generated~~ second identified ~~position~~ code and the ~~newly~~ second generated ~~control~~ position code to create a different encrypted version of the encrypted data string.

Claim 59 (Previously Presented): The method of Claim 3, wherein selecting a predetermined order includes selecting a default order.

Claim 60 (Currently Amended): The method of Claim 10, wherein determining an order based on the frequencies of the 2^n combinations of the n bits of the input data string

includes determining an order based on the relative frequencies of the 2^n combinations of the n bits of the ~~input data string~~binary data.

Claim 61 (Cancelled).

Claim 62 (Currently Amended): An electronic device for encrypting an input data string, including a plurality of bits of binary data, comprising:

a processor configured to receive the input data string for encryption;

a memory configured to include a control code index, the control code index being defined prior to encryption by the processor, the control code index including a plurality of control codes, the control codes having corresponding values each defining respective orders of n bit combinations of binary data,

wherein the processor is operably linked to the memory for determining upon reception of the input data string, an order in which to query the presence of each of two 2^n different configurations of n bits within the input data string, and ~~generates~~ identifies a control code associated with the determined order by access of the control code index ~~in which the generated control code is selected from the control code index independent of specific characteristics of the input data string~~, the processor generating a position code, ~~through the identification of~~ using the identified control code in cooperation with a position code routine associated with the identified with the identified control code to determine positions of each of the two 2^n different configurations of n bits in the input data string ~~in accordance with the determined order~~ by comparing the 2^n different configurations of the input data string with the associated 2^n bit configurations of the identified control code, the comparisons resulting in output values dictated by the position code routine which defines the

generated position code to combine the identified control code and generated the position code as components of an encrypted data string.